Security and Privacy Enabling Solution for Vehicular Networks

Upasana Singh and Pardeep Singh

Computer Science and Engineering
NIT Hamirpur
Hamirpur, India
upasananith@gmail.com, pardeep@nitham.ac.in

Abstract. Vehicular Ad-Hoc Network, better known as VANET is a promising new technology which combines the capabilities of different wireless networks in vehicles enabling Intelligent Transportation System (ITS). Vehicular Ad-Hoc networks provide communication between on-board unit (OBU) already integrated in the vehicles and road-side units (RSUs) consisting of on-board sensors, processing modules, and wireless communication modules. Immense amount of research is going on both by industry and academia. In vehicular communication because of the high speed of vehicles frequent handovers occur and hence there is always a requirement of secure and fast authentication for a seamless handover to take place. In this paper we propose an authentication scheme that will not only provide security and privacy but also will reduce the storage and communication overhead increasing the efficiency.

Keywords: Vehicular Networks, Security, Privacy, Authentication, VANET.

1 Introduction

VANETs are the providers of traffic safety and efficiency including several other applications like public services and infotainment. A large amount of research is being done to enhance the capabilities of VANETs. Among which a significant amount of work is dedicated to communication in vehicular networks. The vehicular communication could be Intra-Vehicular communication or Inter-Vehicle Communication. In Intra-Vehicular communication the On-Board Unit (OBU) communicates with several Electronic Control units (ECU). The Inter-Vehicular Communication could be Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication. For communication in VANETs various wireless technological standards are being developed like Dedicated Short Range Communication (DSRC). Since a rich set of tools are offered to drivers and authorities, a formidable set of exploits and attacks becomes possible. Hence for communicating in vehicular networks every entity has to be authenticated. Also for carrying out communication some keys have to be agreed upon. When a node moves from one RSU's coverage area to another, re-authentication is required in the new security domain, which is called the security handover problem. This realm combines both communication and

V.V. Das, E. Ariwa, and S.B. Rahayu (Eds.): SPIT 2011, LNICST 62, pp. 191–194, 2012.

security.The security of vehicular networks is crucial, because these systems can make anti-social and criminal behavior easier, in ways that will actually endanger the benefits of their deployment. And hence in order to have secure vehicular communication message and entity authentication has to be done, and also message integrity and confidentiality has to be maintained while preserving user's privacy and anonymity.In this paper we have proposed an authentication and key agreement protocol for vehicular networks. The paper is organized in the following way: Section 2 describes the related work. Our proposed solution is given in Section 3 with its security analysis. Finally section 4 concludes the paper.

2 Related Work

In case of vehicular networks a balance has to be made between the security and privacy for its proper functioning. Security and privacy related problems have been discussed by many researchers. While most of them addressed both security and privacy some of them fail to do so. Although communication in vehicular networks has to be real-time constrained, most of the proposals incur communicational overhead. Various techniques have been used to secure vehicular communication like symmetric key cryptography, asymmetric key cryptography, ECC, Id-based cryptography, and some times in combination with some hardware.A secure communication architecture is proposed in [1] based on a public key infrastructure (PKI) and a virtual network controlled by cluster-heads but their approach produces a remarkable overhead and the use of cluster-heads can create bottleneck. The importance of privacy and secure positioning was considered in [4] and proposed the use of Electronic License Plates (ELP) to identify vehicles. Although they recognize the importance of conditional privacy, they do not provide any specific solution to the problem. To the best of our knowledge, there are few articles that consider both security and conditional privacy preservation in VANETs. In this line, [3] gave a foundational proposal of using pseudonym based approach using anonymous certificates and the public key infrastructure (PKI).The anonymous certificates are used to hide the real identities of users. This scheme required extra communication and had storage overhead. Also privacy could be invaded by logging the messages containing a given key and tracking the sender until her identity is disclosed. GSIS presented in [6], is a conditional privacy-preserving scheme using group signatures and ID-based signatures. In it a single membership manager is used to issues secret member keys to the vehicles. The conditional anonymity claimed applies only to the vehicles amongst the peer, with an assumption that the infrastructure points are trusted. An alternative way was proposed in [7] to overcome the limitation of pre-storing a large number of anonymous certificates while preserving conditional privacy. They proposed a group signature based scheme, making an assumption that vehicles and RSUs are able to collaborate actively. Every vehicle gets a short-time anonymous certificate from a RSU after running a Two-round protocol when passing by the RSU. In order to prevent link ability of the messages, the vehicle should change the anonymous certificate regularly by interacting with RSUs. These frequent interactions may affect the network's

efficiency. The group based schemes could not be applied properly due to certain limitation as the difficulty in election of group leader due to the non-availability of a trusted entity among the peer vehicles; also there may be too few cars in the vicinity to create a group.

3 Proposed Algorithm

Vehicular networks consist of several entities. A trusted authority (TA)is one which could be a law enforcement authority (or a group of authorities) that could trace and disclose the identity in case of accident or crime.AAA server is authentication, authorization and accounting server which authenticates the vehicle when it first enters the network and establishes the keys to be used.Road Side Units (RSU) which act as the access points or access routers.And the On-Board Units (OBU)which are installed on vehicles, at RSUs and AAA server.In our solution we will be using terms vehicle and mobile node interchangeably, similarly Access router (AR) and Road Side Unit (RSU) interchangeably. We have divided the Solution in two phases starting with mutual authentication and key agreement phase, next verification phase.Each vehicle is given a unique identity UID and password PSW by the TA. When the vehicle enters a network it enters UID and PSW in the OBU which generates a pseudoidentity ID_A as;ID_A= (UID ⊕ PSW).

3.1 Mutual Authentication and Key Agreement

The AAA server chooses two large primes p and q and keeps them secret, it than computes $n = (p.q)$.When the vehicle first enters the network it sends ID_A to the AAA server. AAA server than computes $J_A = f(ID_A)$ and sends J_A to the vehicle where f( ) is a pseudorandom function. AAA chooses a secret s such that $1 \leq s \leq n-1$ and computes $v = (J_A.s)^2 mod\ n$and makes it publically available. AAA selects and sends a shared secret 'g' to the vehicle. After which both AAA server and vehicle choose respective secret numbers a and b such that $1 \leq a$ and $b \leq g-2$ each co-prime to g-1. They respectively compute $(a^{-1}\ mod\ g-1)$ and $(b^{-1}\ mod\ g-1)$. **AAA server chooses a secret 'k'** such that $1 \leq k \leq g-1$, and computes $(k.a)\ mod\ g$and sends to the vehicle. Vehicle than multiplies the received value by b and sends it to AAA. AAA than multiplies the received value by $(a^{-1} mod\ g-1)$ which undoes its previous multiplication and sends it back to the vehicle. Vehicle than multiplies the received value by$(b^{-1}\ mod\ g-1)$ which results in $K\ mod\ g$. This $K\ mod\ g$ is the shared secret key between the AAA and the vehicle which is used as the Master key (MK). This key will not be used for any kind of encryption it will only be used for deriving handover encryption key. The AAA computes handover encryption key (HEK) using the MK as HEK = (MK||IDMN||IDAR) and sends the HEK to the corresponding AR.

3.2 Verification Phase

Before the vehicle attaches to the new RSU and disconnects from the previous one, previous RSU is responsible to send V's related authentication information to the new

one. Whenever a vehicle enter the vicinity of an RSU and have to communicate its identity must be verified. For verification vehicle sends IDA and x = (JA.r)2 mod n to the NAR(**RSU**) . NAR than randomly select a challenge bit e=0 or 1 and send to vehicle. The vehicle than compute $y=(ID_A.r) \bmod n$ if e=0 and if e=1 than $y = (ID_A.r.s) \bmod n$ and sends it to NAR. NAR than computes J_A from ID_A using f and $y^2 = (x.v^e) \bmod n$. If both the values of y received and calculated are same than the verification is successful.

3.3 Security Analysis

Denial of Service attack: Our proposal suggests a secure binding update authentication scheme using a security association between AR and MN. The scheme provides not only mutual authentication between MN and ARs, but also guarantees secrecy between ARs.Passive attack: Even if the attacker performs a passive attack, hecan't succeed as after verification both vehicle and the RSU will compute their session keys based on their secret shared information that attacker can not compute. Moreover the session key is computed by both vehicle and the RSU instead of transmitting. Therefore the proposed protocol is safe against the passive attack.Man in middle attack: It is a kind of active attack. Since no information about the secret key is revealed so the solution is safe against the man in middle attack. Even if the adversary intercepts the signals 'g' sent by the RSU in the verification process the adversary would not be able to face the real time challenge, so the solution is safe against the man in middle attack.

4 Conclusion

Vehicular networks are the vital solution to secure and efficient transportation system proving different types of applications to the vehicles. In order to take full advantage of the vehicular networks the communication must be secured meeting all the security requirements. Our proposed solution provides security and privacy both using symmetric key cryptography reducing the computation and storage required.

References

1. Blum, J., Eskandarian, A.: The threat of intelligent collisions
2. Gollan, L., Meinel, C.: Digital Signatures for Automobiles. Technical Report, Institute for Telematike 6(1), 24–29 (2004)
3. Raya, M., Hubaux, J.: Securing vehicular ad hoc networks. Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks 15(1), 39–68 (2007)
4. Lin, X., Sun, X., Ho, P.: GSIS: A secure and privacy preserving protocol for vehicular communications. IEEE Trans. Vehicular Technology 56(6), 3442–3456 (2007)
5. Lu, R., Lin, X., Zhu, X.: ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications. In: IEEE INFOCOM 2008, pp. 1229–1237 (2008)
6. Zhang, C., Lu, R., Lin, X.: An efficient identity based batch verification scheme for vehicular sensor networks. Journal IEEE INFOCOM 2008, 246–250 (2008)